ПАСИВНІ МЕТОДИ ЗАХИСТУ ХМАРНИХ ОБЧИСЛЕНЬ В AMAZON AWS

Носко С.В., Зиков І.С.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

На сьогоднішній день хмарні обчислення є перспективним напрямком сучасних інформаційних технологій. Хмарні обчислення (cloud computing) – це технологія розподіленої обробки даних, в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс, тобто робочий майданчик на віддаленому сервері.

Організації використовують хмарні технології в різноманітних моделях обслуговування (SaaS, PaaS, та IaaS) та розробницьких моделях (Private, Public, Hybrid, та Community). Є ряд питань/проблем, пов'язаних з безпекою хмарних обчислень, але ці питання діляться на дві великі категорії: питання безпеки, з якими стикаються під час використання хмарних послуг (організації, які надають програмне забезпечення, платформи, чи інфраструктуру як послуги через використання хмарних технологій) і питання безпеки, з якими стикаються їх клієнти (компанії або організації, які розгортають додатки або зберігають дані на хмарі). Відповідальність йде в обох напрямках, тобто: постачальник повинен гарантувати, що їх інфраструктура знаходиться в безпеці і що дані та додатки клієнтів захищені, в той час як користувач повинен вживати заходи, щоб зміцнювати їх застосування, використовувати надійні паролі і перевірку автентичності.

Можна виділити активні і пасивні методи захисту хмарних обчислень. Активні полягають в постійному опитуванні інфраструктури з метою проведення якогось аналізу, але це є досить затратно як в плані навантаження на ресурси так і в ціні.

Специфікою даної роботи є вирішення задач аналізу і безпеки дій користувача над інфраструктурою методом пасивного захисту, записуючи всі виклики AWS API в лог-файли. Записана інформація включає в себе ідентифікацію джерела, яка вчинила виклик API, час виклику API, IP-адреса джерела, яка вчинила виклик API, параметри запиту, а також елементи відповіді, повернуті сервісом AWS. Історія викликів API AWS уможливлює проведення аналізу безпеки, відстеження змін ресурсів і аудит відповідності. Також було реалізовано механізм, який подібно тригеру в базі даних визивається і моментально доставляє результат аналізу на пошту власнику віртуальних ресурсів.

Отже, було запроповано новий метод пасивного захисту хмарних обчислень, який базується на використанні лог-файлів і дозволяє швидко виявити причину несправностей. Від аналогів відрізняється своєю дешевизною і невисоким навантаженням на інфраструктуру, адже не пінгує постійно віртуальні ресурси. Для користувачів це дасть ефективний інструмент для аналізу своїх ресурсів і базується на стеку технологій Amazon AWS, шо є дуже популярним серед провайдерів хмарних обчислень.